IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 5, May 2024

DOI: 10.17148/IARJSET.2024.11577

Secure Logistics using IoT and Cryptography against attacks

Raghavendra Babu T M[1], Aishwarya K M[2], Hemana M[3], Anusha M C[4], Bhoomika C S[5]

Assistant Professor, Department of Computer Science and Engineering, PES College of Engineering, Mandya, India[1]

B E Students, Department of Computer Science and Engineering, PES College of Engineering, Mandya, India[2-5]

Abstract: In contemporary logistics operations, technology plays a pivotal role in replacing antiquated systems. This article proposes a comprehensive solution for securing goods in transit using a integration of cryptography and IoT technology to mitigate threats. In our proposed system cryptographic measures at logistics doors, requiring authorized personnel to give a hash function, specifically utilizing the MD5 encryption algorithm, to inspect the goods. It employs encryption technique to secure the passwords associated with access points along the transportation route. Upon door opening, an alert message is deliver to the sender via the Blynk App, enabling real-time tracking and location verification. Additionally, the system incorporates weight sensors to detect any tampering to the transported goods. Upon detecting such anomalies, the system triggers alarms or sends the alert to relevant stakeholders. The stakeholder can remotely access the system via the Blynk app to track the location. This integrated approach ensures the protection of goods throughout the journey, safeguarding against potential cyberattacks and theft incidents.

Keywords: Cryptography – MD5 algorithm, Weight sensor, Microcontroller (NodeMCU), Blynk application

I. INTRODUCTION

Rapid changes in technology. Old technologies are continuously being replaced by new and sophisticated ones. Enable the people for new technology to have their work done efficiently such as IoT and Cryptography. The IoT has become an arising key technology for future, in which a myriad of sensors, actuators, and smart objects in our daily life are connected to the Internet. These sensors and actuators (e.g., surveillance cameras, home appliances, and environment monitoring sensors) are typically equipped with different kinds of microcontroller, transceivers, and protocols for communications of sensing and control data. These real life objects, either sensors or actuators, are connected with each other to transfer their sensed data to centralized servers, where information is collectively stored and made available for particular users with proper access rights.

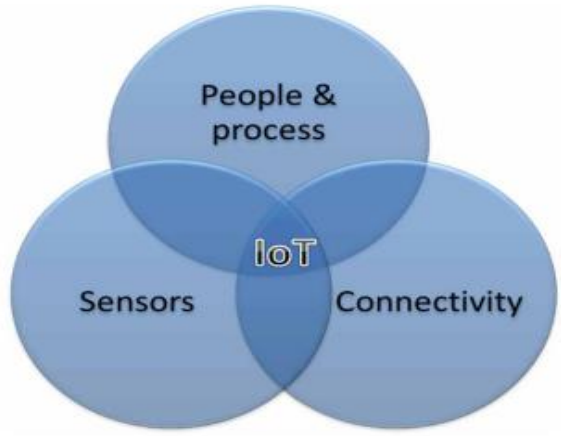


Fig 1. IoT Environment components

Cryptography is the technology consisting the principles and methods of transforming an intelligible message into one that is unintelligible, and then retransforming that message back to its original form. Plain message - The original intelligible message.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 5, May 2024

DOI: 10.17148/IARJSET.2024.11577

Cipher message - The transformed message. Cipher - An algorithm for transforming an intelligible message into one that is unintelligible by transposition and/or substitution methods. Key - Some critical information used by the cipher, known only to the owner & receiver. Encipher (encode) - The process of transforming plaintext to cipher text using a cipher and a key. Decipher (decode) - The process of transforming cipher text back into plaintext using a cipher and a key.

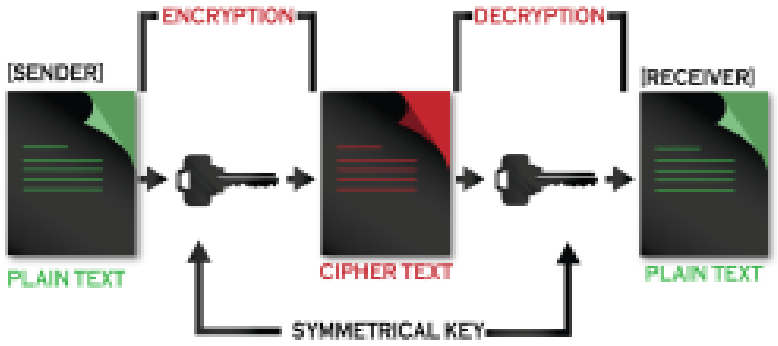


Fig 2. Block diagram of cryptography

Attacks are deliberate attempts to compromise the confidentiality, integrity, or availability of computer systems, networks, or data. They can target individuals, organizations, or even entire nations. Attacks can attends to financial loss, data breaches, reputation damage, and disruption of services. Attackers often exploit vulnerabilities in software, hardware, or human behaviour to achieve their goals. It's significant to stay vigilant, employ robust security measures, and regularly update systems to mitigate the risks posed by attacks.

In this proposed system, we can reduce the attacks using Iot and Cryptography which includes several strategies such as Implement Strong Encryption, Integrity verification, Continuous Monitoring and Updates.

1. **Implement Strong Encryption**: Use robust cryptographic algorithms to encrypt sensitive data transfers between IoT devices and networks, making it difficult for attackers to intercept and decipher the information.

2. **Integrity Verification**: Use cryptographic approaches such as digital signatures or message authentication codes to validate the integrity of data transfers between IoT devices, detecting any unauthorized modifications.

3. **Continuous Monitoring and Updates**: Regularly monitor IoT devices and networks for security vulnerabilities and apply patches and updates promptly to address any identified weaknesses and protect against emerging threats.

II. LITERATURE REVIEW

Amit Singha, Nasirul Mumenin, Nahid Ibne Akhter, Md. Shahadat Hossain Moon, and Mosabber Uddin Ahmed: Authors says that several research efforts have focused on developing Iot, cryptographic solutions for logistics, many problems remain, particularly in conditions of object integrity and service trustworthiness. Due to the huge range of potential cyber and physical security risks, these issues are difficult to address successfully. Wireless sensor networks (WSN) can be used to monitor meteorological factors in an agricultural area in this case. This article offers a safe communication system for WSN where each communication step is encrypted using appropriate cryptographic algorithm, MUMAP and TWINE are both lightweight methods, they may be deployed economically with limited resources [1]. Waseem Hamdoon, Ahmet Zengin: Authors discussed that an Internet-of-Things-based architecture for smart irrigation by developing a prototype with a controller unit, water pumps, and sensors. These systems monitor the soil's irrigation needs and detect the right amount based on sensor data [2]. Gabriela Ioana Enache: Author says that the insights into the main cybersecurity concerns affecting the logistics industry and explain viable ways for reducing these risks through a thorough study of recent research. The IoT has made it possible to use smart devices that can gather and analyze massive volumes of data in real time, giving logistical operations valuable information.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 5, May 2024

DOI: 10.17148/IARJSET.2024.11577

Security measures for logistics systems will grow more dependent on cybersecurity, IoT, 5G, big data, and cloud computing as logistics organizations continue to adopt digital technologies [3]. Mohan, S: Author describes the terms Industry 4.0 and Logistics 4.0 as two of the most important trends in production and logistics. It characterizes the big chances of this development.

The paper gives an overview about important solutions in this area. Some new solutions are discussed according to material sciences, as it is also very important to develop and use new materials, which help to create smart solutions. Smart materials are created in the areas of e.g. laminated, composite and functionally graded materials, thermal and piezoelectric actuation, active and passive damping, vibrations and waves in smart structures [4].

Glistau, E. & CoelloMachado. NI: Authors describes the importance of Big Data in Logistics based on scholarly articles and it also highlights different challenges faced by logistics operation by employing Big Data and how Logistics Cost Optimization is achieved using Big Data. Moreover, Big Data in Logistics is an emerging aspect which has both pros and cons [5].

Gligor, D.M. and Holcomb, M.C: Authors discussed the duty of logistics capabilities in accomplish supply chain flexibility through a multi-disciplinary review of the relevant research. The literature on logistics capabilities was also examined to identify the various elements that contribute to supply chain flexibility [6].

III. PROBLEM STATEMENT

Here to develop a robust system where cryptography will be employed to authenticate access, ensuring that logistic compartments can only be monitored by authorized personnel. Simultaneously, IoT devices will be utilized to monitor and send real-time alerts to the owner in case of any unauthorized access attempts or potential thefts. The combination of these technologies is expected to significantly mitigate the hazard of attacks on logistic systems, thereby safeguarding valuable goods throughout their journey. This project seeks to design, implement, and validate an integrated IoT and cryptographic solution to achieve a secure and efficient logistic system.

IV. EXISTING SYSTEM

A WSN is interconnected sensor nodes that communicate wirelessly to collect data about the surrounding environment. WSN can be utilized to monitor meteorological factors in an agricultural area. In the existing system offers a safe communication system for WSN where each communication step encrypted using cryptographic algorithm with authentication and encryption of data. The security architecture of WSNs relies heavily on cryptographic methods.

In this manuscript, a safe WSN communication framework is developed which uses an ultra-lightweight authentication mechanism, MUMAP (modified ultra-lightweight mutual authentication protocol) for sensor node to sink node authentication and lightweight cryptographic algorithm, TWINE for security sink nodes to base station communication.

Advantages:

➢ Integrity: Data will be transmitted from sensor nodes to sink nodes based on authentication.
➢ Mutual Authentication: Both the valid sensor node and the sink node should communicate and test each other.
➢ Confidentiality: The sink nodes aggregate data packets are encrypted. An attacker must first decrypt the data in mandate to get it. The encryption method in use impenetrable to cyber-attacks.
➢ Forward security: If the sensor node is compromised, forward authentication is required to safeguard the sink node's previous communication with the sensor node.

V. PROPOSED SYSTEM

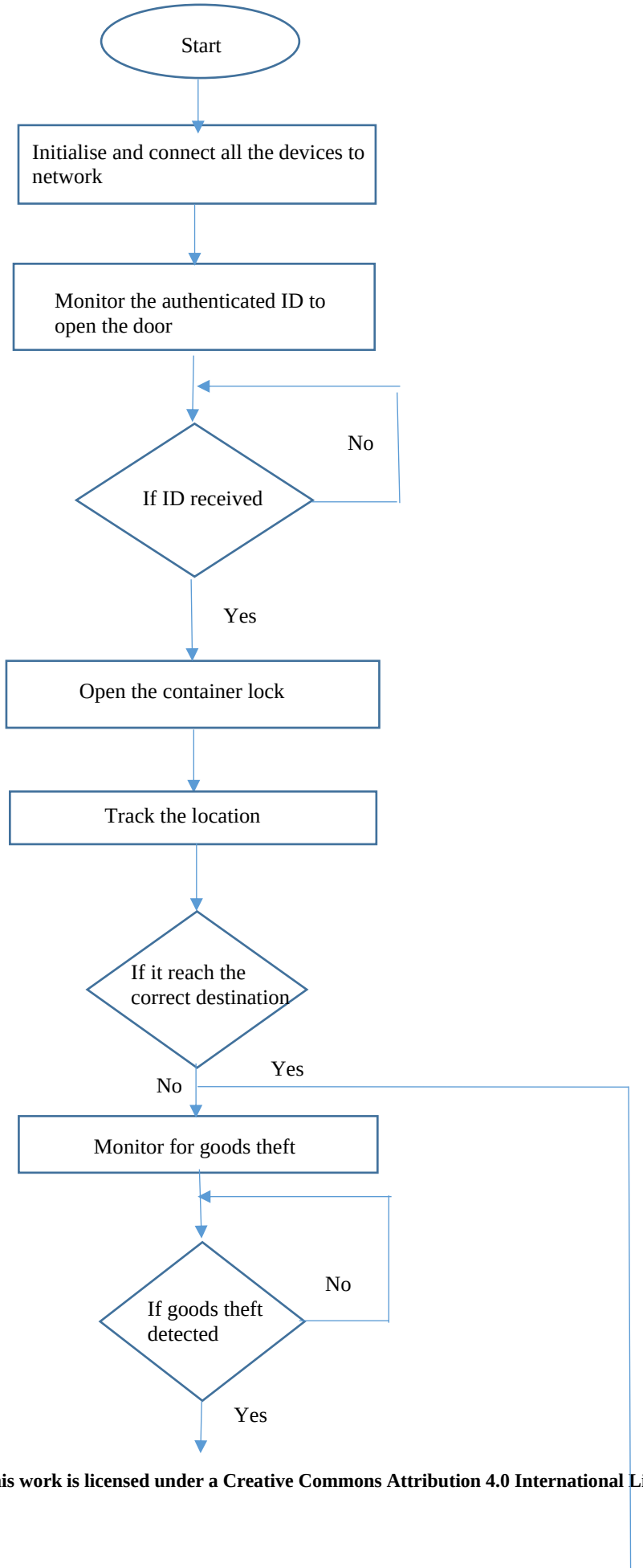
In our proposed system, functionality is to secure and monitor the logistics which is travelling between source and destination using IoT and Cryptographic technique.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 5, May 2024

DOI: 10.17148/IARJSET.2024.11577



IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 5, May 2024

DOI: 10.17148/IARJSET.2024.11577

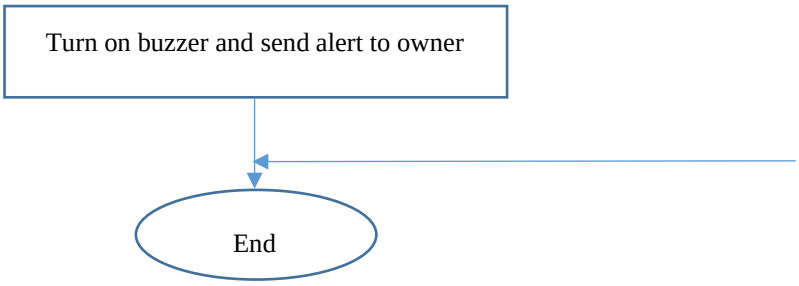


Fig 3: Flow diagram of Secure logistics using IoT and Cryptography

VI. IMPLEMENTATION

The developed model is built and integrated as shown in the Fig 4 and Fig 5. The logistics container is secured with a cryptographic authentication system using MD5 algorithm and IoT sensors. If someone needs to open the container, they must provide correct administrative credentials (username and password). This feature protects against unauthorized access during transit.

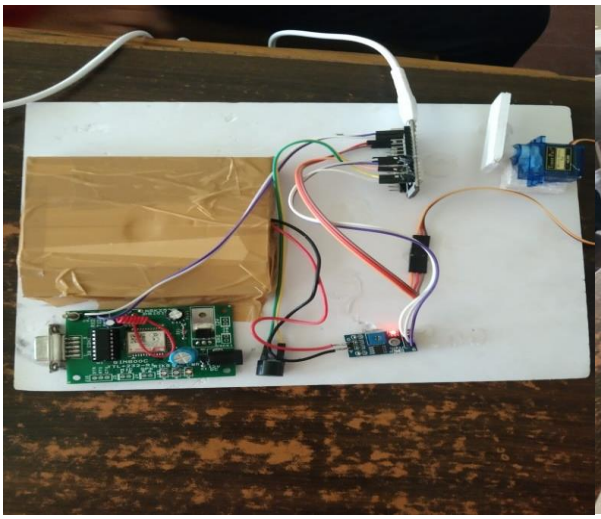


Fig 4: High-angle view of prototype model

Fig 5: Lateral view of prototype model

When the door is opened legitimately, notifications are issued to the owner or admin, ensuring they are conscious of the access event. This helps in keeping track of when the logistics are accessed. The owner can track the location of the logistics in real-time through a mobile app. If the container deflect from its intended path or reaches its destination, the owner receives updates and can take necessary actions if needed. If someone attempts to tamper with the contents or test the security of the container, a sound buzzer is triggered, and an SMS alert is issued to the owner. This immediate notification allows for quick response to potential security breaches. The system uses a GSM module to communicate alerts and notifications, ensuring the owner is always informed about the status of the container, whether the door is open, and the safety of the contents.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 5, May 2024

DOI: 10.17148/IARJSET.2024.11577

VII. RESULTS

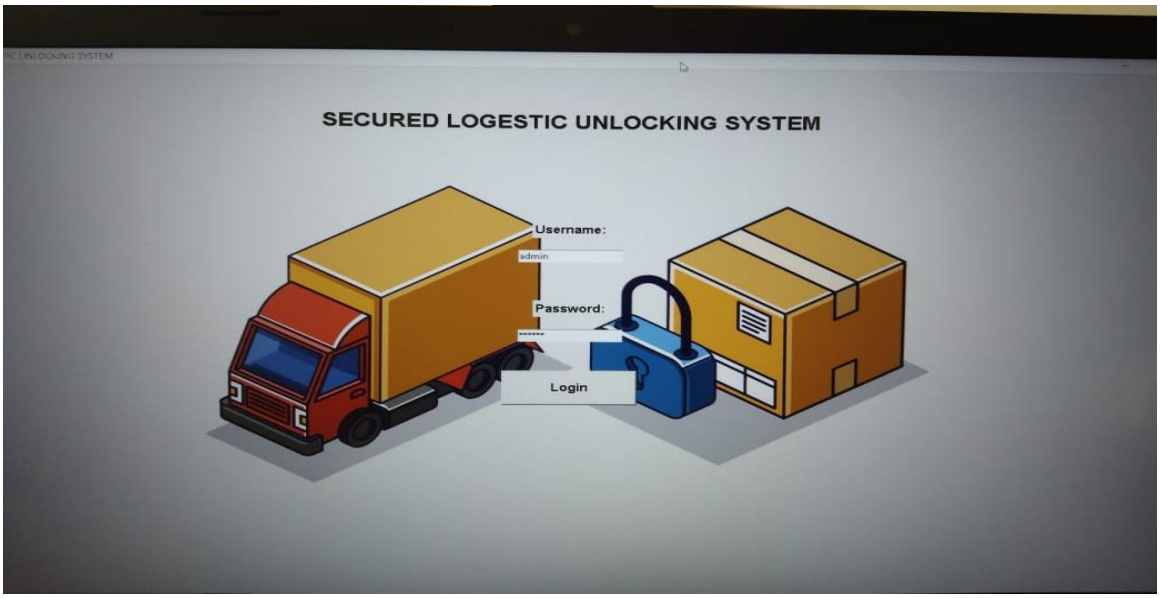


Fig 6: Logistic unlocking system

The Fig 6 shows the implementation of the MD5 cryptographic algorithm to secure the authentication process. Develop a application where the logistical door only opens after verifying the correct admin username and password.

Fig 7: Blynk notification of current status

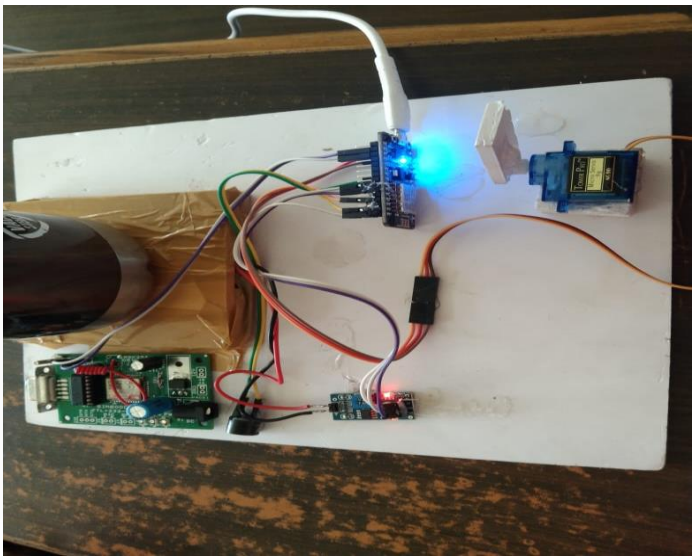


Fig 8: Logistic condition when door open

Fig 7 shows that we program the system to communicate with the Blynk app, allowing real-time monitoring and control. Develop an interface on the Blynk app to display the door's status and the security state of the items inside. Fig 8 shows the hardware setup in which the door will open after entering the correct username and password in the application.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 5, May 2024

DOI: 10.17148/IARJSET.2024.11577

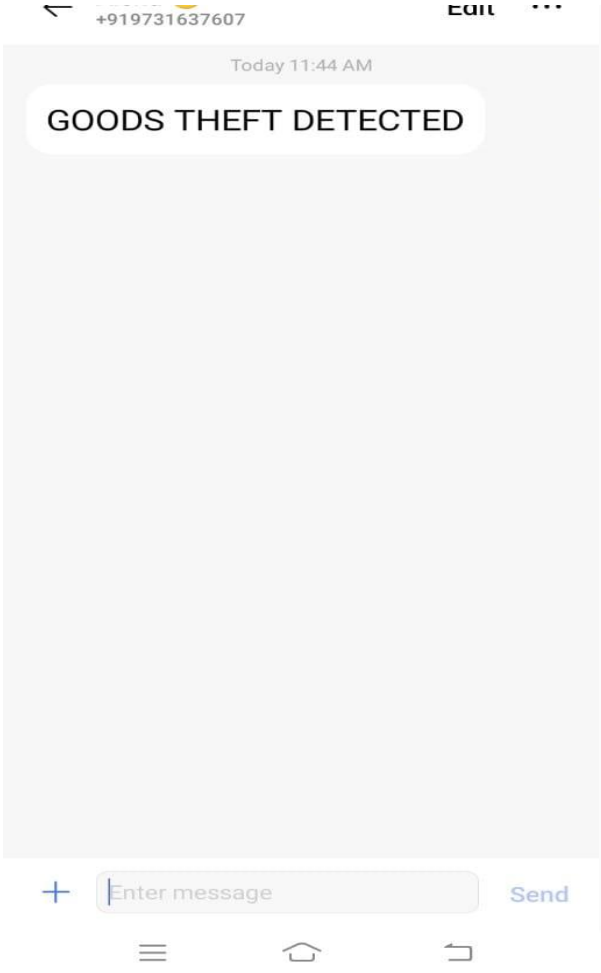


Fig 9: SMS when theft detected

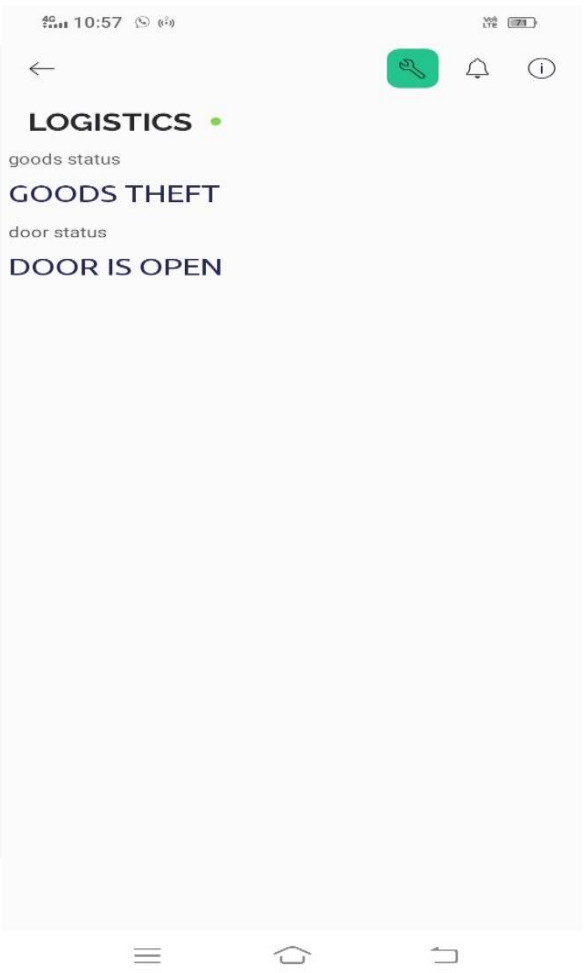


Fig 10: Blynk notification when theft detected

We implement logic for detecting theft events based on sensor data and triggering alerts accordingly. If theft occurs, text message is send to the owner via GSM module (Fig 9) and goods status also displayed in the blynk application as shown in the fig 10.

VIII. CONCLUSION

Comprehensive approach to securing logistics using IoT and cryptography. By combining IoT devices with cryptographic algorithms, we ensuring authorized access to logistic doors while also providing notifications for added security. This not only improves safety mechanisms but also facilitates real-time monitoring, ensuring confidentiality of the logistics process. It's a robust solution against attacks.

IX. FUTURE ENHANCEMENT

We will implement advanced mechanisms and technology tools to ensure security when the prescribed location does not sync the destination. This will involve developing protocols for the owner to take proactive measures in such circumstances, enhancing the overall security of the project or model.

Additionally, using a single-layer sensor for object deployment between source and destination, we will upgrade to double or triple layers of sensors within the system. This development will significantly improve scalability and usability, providing a more robust solution for the project objectives.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 5, May 2024

DOI: 10.17148/IARJSET.2024.11577

REFERENCES

[1] Amit Singha, Nasirul Mumenin, Nahid Ibne Akhter, Md. Shahadat Hossain Moon, and Mosabber Uddin Ahmed, Title: A Lightweight Cryptographic Scheme to Secure WSNs in Agriculture, pp.615-624, March 2022.

[2] Waseem Hamdoon, Ahmet Zengin, and Title: A Proposed Smart Irrigation Management System based on the Iot and Cloud Computing technologies, June 2023.

[3] Gabriela Ioana Enache, Title: Logistics Security in the Era of the Big Data, Cloud Computing and IoT, pp.188-199, July 2023.

[4] Mohan, S. (2017). Big Data: Transforming Logistics and Supply Chain. International Journal of Pure and Applied Mathematics. Volume 117 No. 20, 911-916.

[5] Glistau, E. & CoelloMachado. NI. (2018). Industry 4.0, logistics 4.0 and materials-Chances and Solutions. Trans Tech Publications. Vol 919, pp. 307-314.

[6] Gligor, D.M. and Holcomb, M.C. (2012), "Understanding the role of logistics capabilities in achieving supply chain agility: a systematic literature review", Supply Chain Management: An International Journal, Vol. 17 No. 4, pp. 438-453.